Chapter 4

Communications

CONTENTS PAGE

PRINCIPLES AND DEVELOPMENTS IN COMMUNICATIONS SYSTEMS

Communications are essential for gathering data and planning operations and supervising performance. Communications are also essential for performing C2 functions. Effective management of DISCOM functions depends on adequate communications to keep abreast of changing situations and requirements.

The DISCOM relies on its organic communications assets and the division signal battalion for communications support. A large number of units operate in the DSA. This density factor may require support units to find alternate methods for communication. The length of transmissions and the accuracy with which they are sent directly affect the support mission. CSS planners should consider using couriers and wire communications as alternatives for getting the support mission done. These alternatives lessen the security risk of substantial radio use.

Communications equipment and systems in the corps and division are changing. The current area communications system is described below. This system will be replaced by the MSE system. Current FM (AN/VRC-12 series) radios and AM (AN/GRC-106) radios will be replaced by the SINCGARS and the improved high frequency radios.

These changes will affect the DISCOM in the area of connectivity to the area system. The command operations company of the division signal battalion installs, operates, and maintains the automatic telephone and switchboard facilities for access to the area system. The company also installs and maintains local subscriber circuits. Under MSE, DISCOM personnel will run wire from unit locations to the MSE interface point. The amount of wire needed is based on the dispersion requirements of the particular situation.

With the deployment of MSE, the wire-laying for all units will have to be covered by unit SOP. It must cover who does it and in what priority, The actual communications means will remain essentially the same. The DISCOM will depend on combat net radios and wire to access the area communications system. Automated hardware systems terminals will be subscribers to the area system via wire.

CURRENT AREA SYSTEM

Figure 4-1 depicts the current area communications system. The command operations company of the division signal battalion provides communications support for the DISCOM HHC/MMC. The following is a list of the communications facilities and services provided by this company:

- Installs and operates a radio teletypewriter terminal in the division's general purpose net.
- Installs and maintains cable and wire for local telephone circuits. DISCOM personnel will help the signal battalion personnel during the initial installation.
- Installs and operates the multichannel terminals in the division communications system.
- Installs, operates, and maintains automatic telephone and switching facilities. These facilities provide

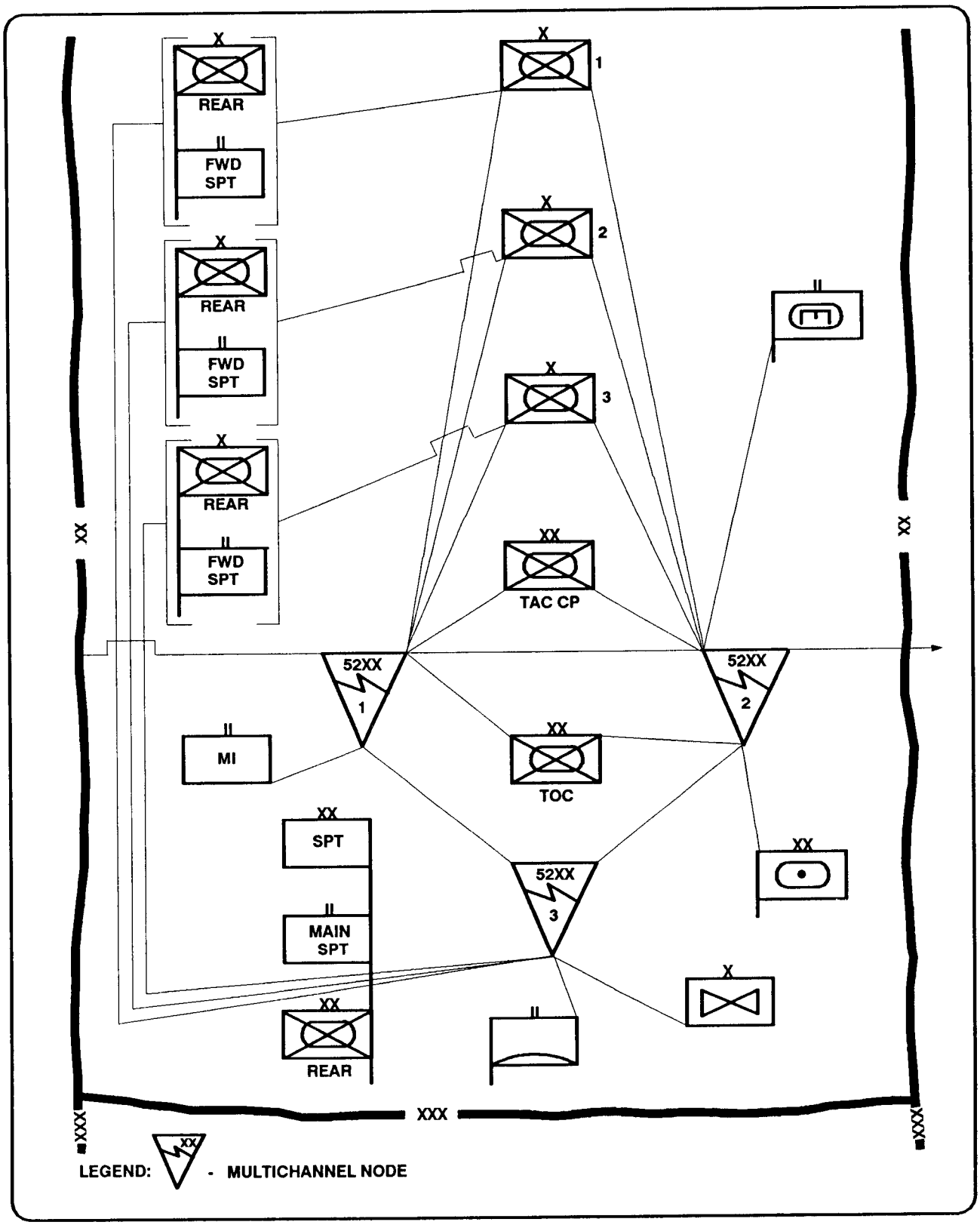

Figure 4-1. Sample armored/mechanized infantry division multichannel diagram (current area system).

access to the area system and local telephone subscriber circuits (DISCOM switchboard).

- Provides telephone equipment for the DISCOM HHC and DMMC (see Figure 4-2).
- Provides a record traffic receiving and distribution center.
- Installs and operates a net radio interface facility for single channel voice radio access to the division's telephone system.

Telephone installer-repairer personnel install and maintain local telephones for the DISCOM headquarters.

Under MSE, the existing 2-wire switchboards and telephones will not be compatible with the 4-wire digital system. The DISCOM HHC, however, will keep the switchboard for internal operations and for local security.

MOBILE SUBSCRIBER EQUIPMENT AREA COMMUNICATIONS SYSTEM

MSE is the area common user voice communications system within the corps. It is the primary means for command and control from the corps rear to brigade rear. It will be deployed from the corps rear boundary forward to the maneuver battalion main CP. The MSE system is comprised of four functional areas:

- Area coverage.
- Wire subscriber access.
- Subscriber terminals.
- Mobile subscriber access.

AREA COVERAGE

Area coverage means that MSE provides common user support to a geographic area, as opposed to dedicated support to a specific unit or customer. Figure 4-3, page 4-5, shows the deployment of area nodes across a corps area. These nodes are called node centers. These centers are shown in Figure 4-4, page 4-6. They are under the control of the corps signal officer,

At division level, the signal battalion operates four of these nodes. The small and large node extension switchboards are connected to these nodes via line-of-sight radios. The following switchboards are organic to the division signal battalion:

- 16 SEN switchboards capable of supporting 26 to 41 subscribers each.
- 1 LEN switchboard capable of supporting 176 customers.

Figure 4-5, page 4-7, shows a typical deployment of switchboards within the division. The G3 will determine the location of switchboards based on the recommendations of the division C-E officer.

The C-E officer considers the commander's intent, customer requirements, and other factors of METT-T. Switchboard locations cannot be consistently related to specific units.

WIRE SUBSCRIBER ACCESS

Wire subscriber access points will provide the entry point (interface) between fried subscriber terminal and the MSE area system. The fixed subscriber terminal and its equipment are owned and operated by the users. The signal units operate the MSE area system. Figures 4-6 and 4-7, page 4-8, show the MSE switchboard configurations. It is through one of these configurations that the DISCOM HHC/MMC ties into the area system,

The following are the two types of interface points:

- The signal distribution panel (junction box) J1077. Each panel can provide up to 13 subscriber access points.
- Remote multiplexer combiners which provide up to eight subscriber access points.

Beyond these two interface points, the using units are responsible for the installation and operation of fixed subscriber terminal instruments. They are also responsible for the installation and maintenance of the WF 16 field wire from the instruments to the interface points into the area system.

SUBSCRIBER TERMINALS (FIXED)

Subscriber terminals used by the DISCOM are digital nonsecure voice telephones. These provide full duplex digital, 4-wire voice as well as a data port for interfacing the AN/UXC-7 facsimile (informal record traffic). The TACCS computers (for CSS STAMIS), the AN/UGC-144 (single subscriber terminal for formal record traffic), the unit-level computers (for the unit-level logistics STAMIS), and the ATCCS (for the CSSCS) will interface through these terminals. Figure 4-8, page 4-9),

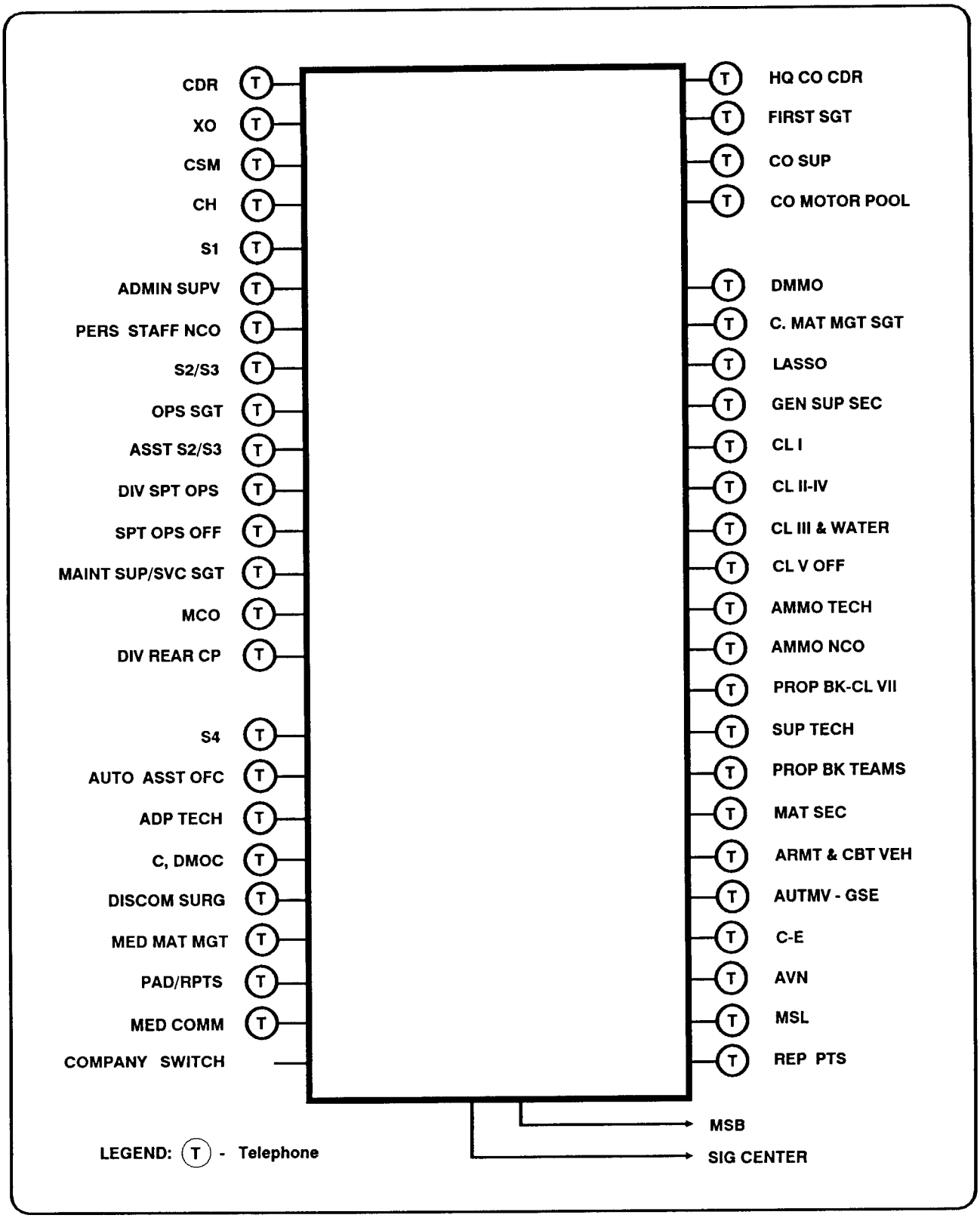

Figure 4-2. DISCOM HHC/MMC wire net.

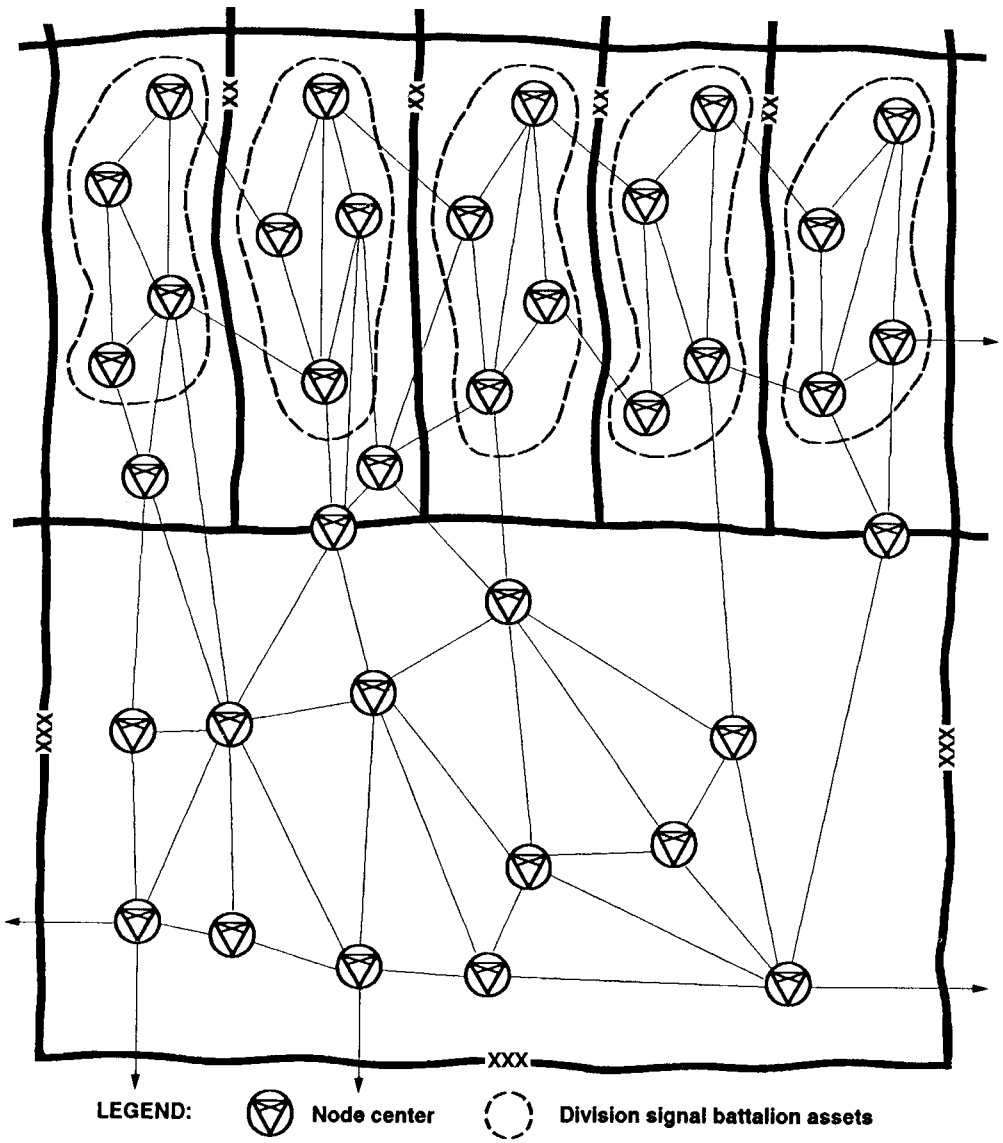

Figure 4-3. Deployment of area nodes (MSE).

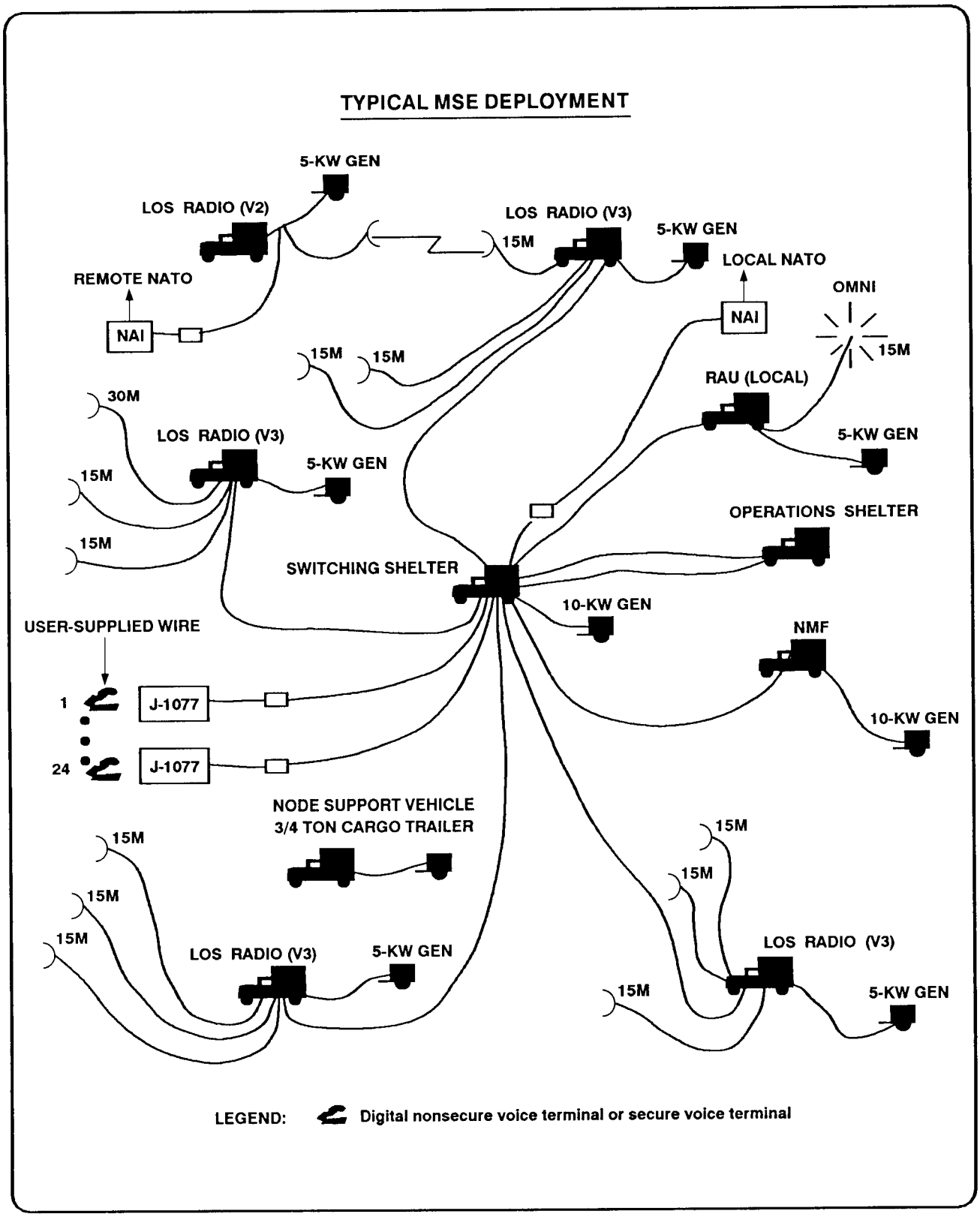

Figure 4-4. Node center.

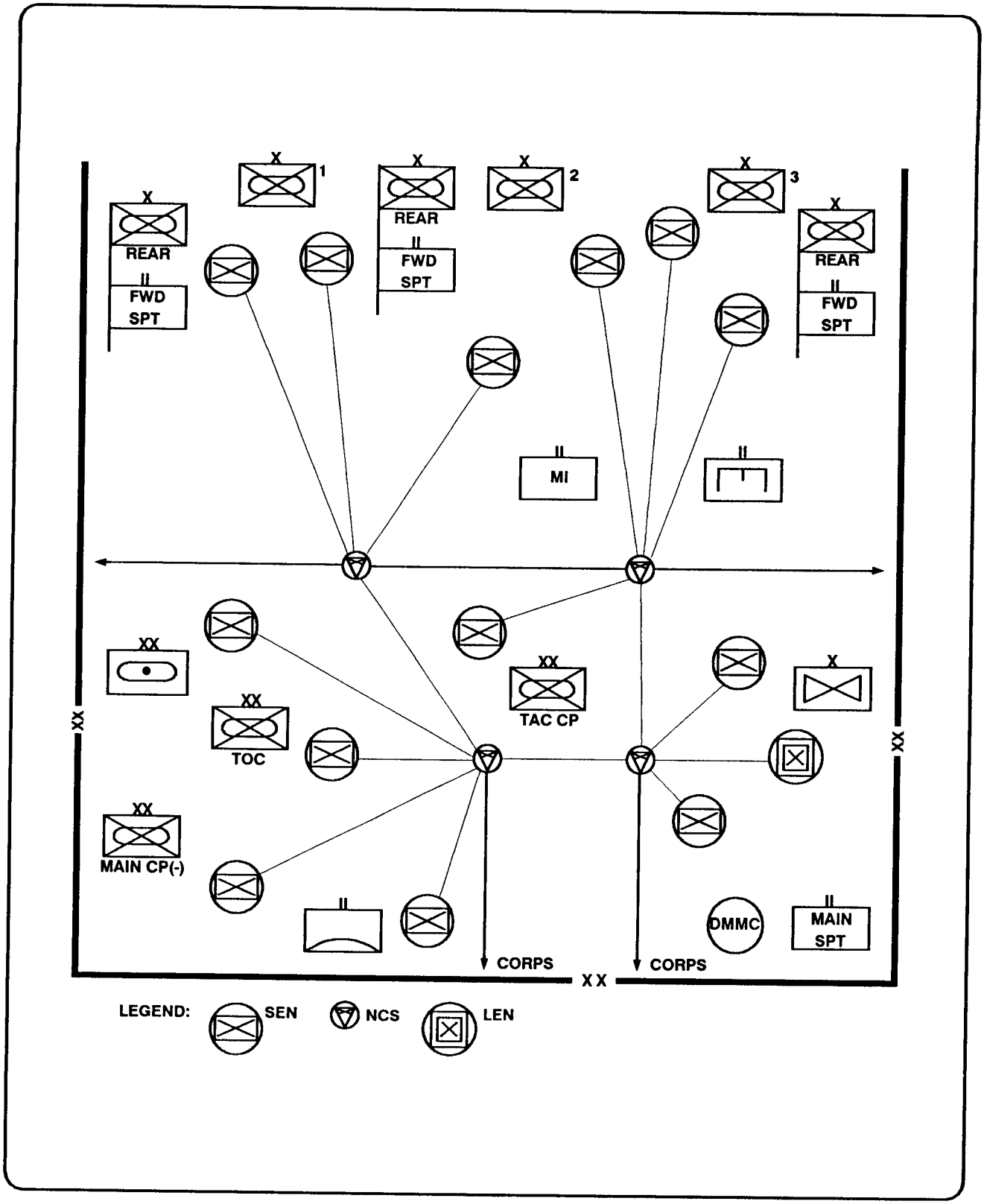

Figure 4-5. Sample division deployment of SEN and LEN switchboards.

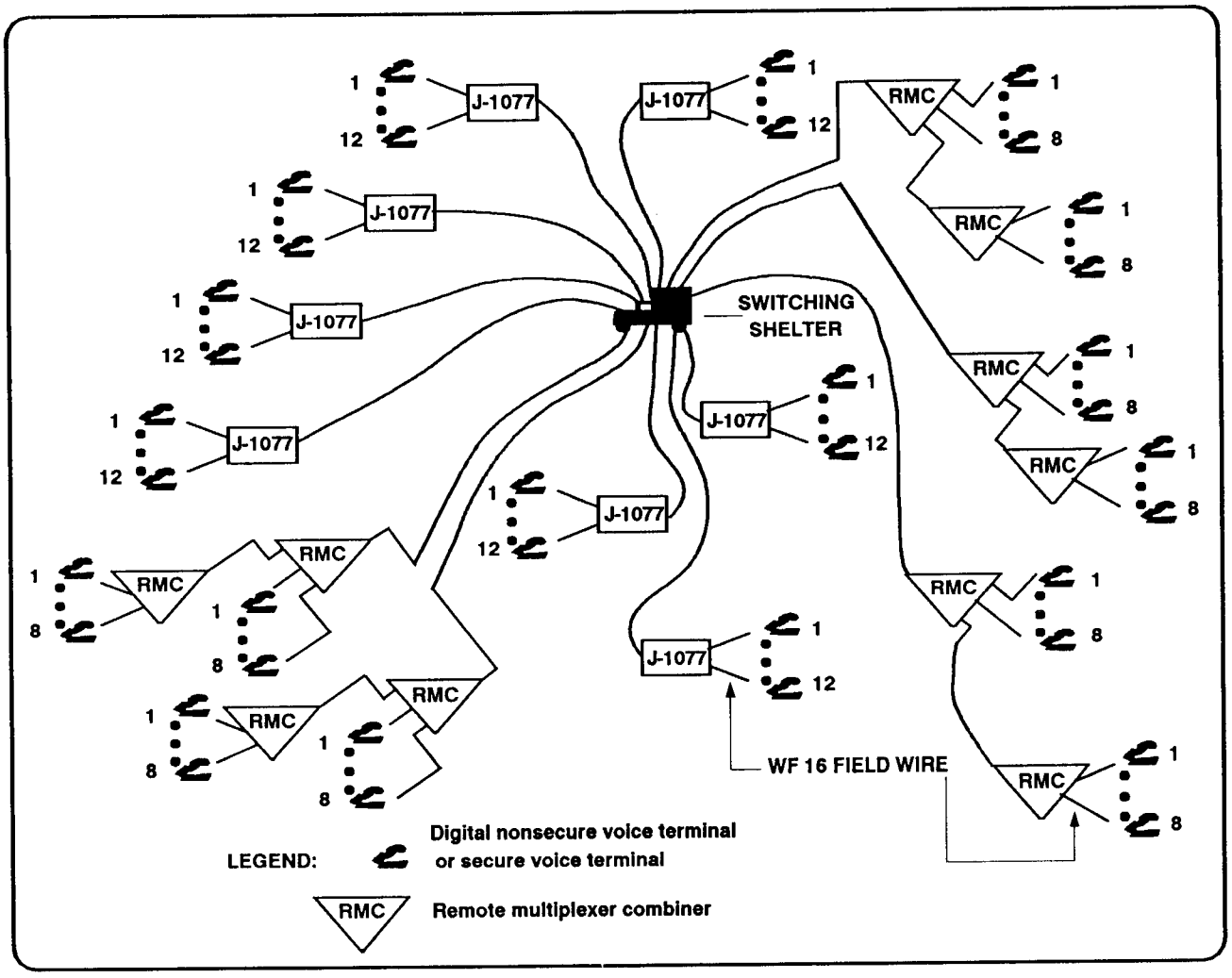

Figure 4-6. LEN switchboard interface.

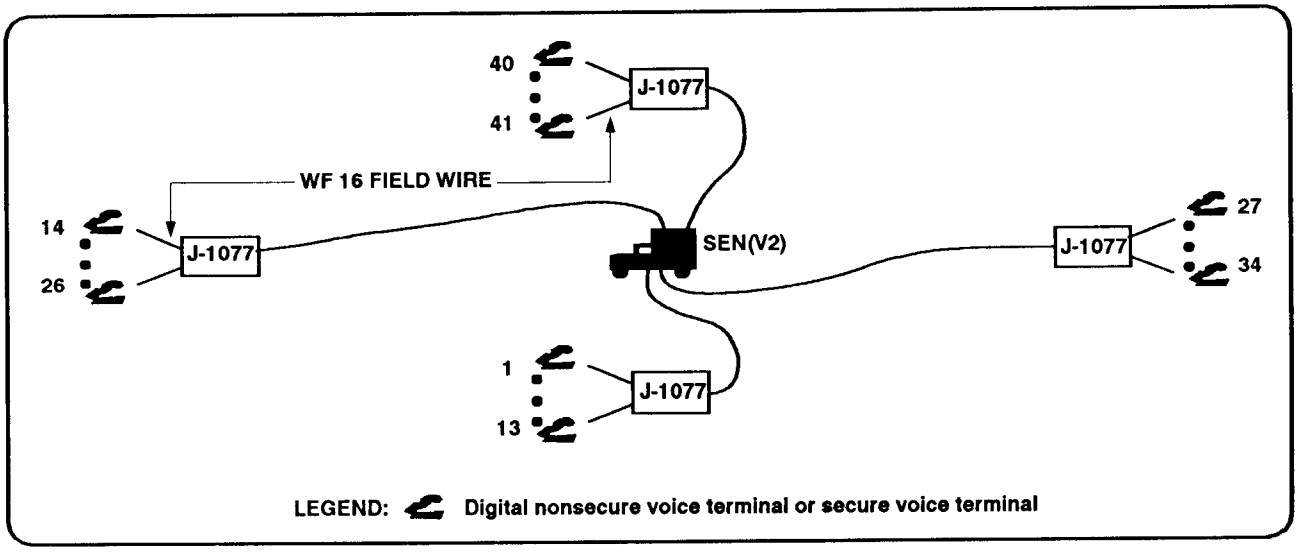

Figure 4-7. SEN switchboard interface (V2).

USER	DEVICE	DATA TERMINAL	STAMIS
CDR	⟳ ○		
XO	○		
S1 (2 ea)	⟳ ○	TACCS, FAX - SST	SIDPERS
S2/3	⟳ ○		
PLANS/INTEL (2 ea)	⟳ ○	*AC - TCP, FAX	MCS
COMM BR	○		
SPT OPS	⟳ ○	ATCCS , FAX	CSSCS
MCO	⟳ ○	TACCS	DAMMS-R
AUTO ASST OFC	○	TACCS (2 ea) , ULC (2 ea)	SYSTEMS SUPPORT
S4	○	ULC	ULLS -S4
MED OPS	⟳ ○	ATCCS	MED - PAR, MED - BLD
MED MAT	○	ATCCS	MED - LOG
PAD/RPTS	○		
DMMC OFC (3 ea)	⟳ ○	ATCCS, FAX	CSSCS
CL I BR	○		
CL II - IV BR	○	TACCS	SARSS-2A
CL III AND WTR SUP BR	○		
CL V SUP SEC (3 ea)	⟳ ○	TACCS	SAAS-DAO
PROP BK - CL VII SEC	○		
DOC CON	○	TACCS (7 ea)	SPBS-R
MGT- ASSET ACCT	○	TACCS	SPBS-R
RPT BR	○		
MAT SEC	○	TACCS	SAMS-2
ARMT- CBT VEH	○		
AUTMV - GSE	○		
C - E	○		
AVN	○		
MSL	○		
REP PTS	○	TACCS	SARSS-2A
HQ CO	○	ULC	ULLS
LASSO (2 ea)	○	DAS-3	DS4
CHAPLAIN	○		

LEGEND: ⟳ MSRT ○ DNVT * Interim equipment

Figure 4-8. DISCOM subscriber terminal assignment, fixed and mobile.

portrays the assignment of this equipment for the DISCOM HHC/MMC.

MOBILE SUBSCRIBER TERMINAL

The MSE mobile subscriber terminal is the AN/VRC-97 mobile subscriber radiotelephone terminal. This MSRT consists of a very high frequency radio and a digital *secure* voice terminal. This is a vehicle-mounted assembly. The MSRT interfaces with the MSE system through a radio access unit. The primary use of the MSRT is to provide mobile subscribers access to the MSE area network. Figure 4-9 portrays a typical MSRT interface into the area system. RAUs are deployed to maximize area coverage and MSRT concentrations. MSRTs can also operate in CPs to allow access to staff and functional personnel. Figure 4-8 represents assignment of MSRTs in the DISCOM, The MSRT user will have a KY68 telephone connected to the radio mounted on his vehicle. As long as the radio unit has line-of-sight contact with the RAU, it has connection into the area system. The operational planning range is 15 kilometers from any RAU.

COMBAT NET RADIO SYSTEM

The combat net radio structure is designed around three separate radio systems; each has different capabilities and transmission characteristics. The three systems are –

- SCOTT.
- IHFR.
- SINCGARS.

SCOTT is a stand-atone transportable tactical satellite communications terminal. The other two systems, IHFR and SINCGARS, will provide means of voice transmission of C2 information. They will also provide means for data transmission. This will be necessary if data transfer requirements cannot be met by the MSE system.

Current CNR equipment in the DISCOM consists of the AN/GRC-106 and the AN/VRC-12 series radios. These will be replaced by IHFR and SINCGARS series respectively. SINCGARS ***is*** a new family of VHF-FM radios. These radios are designed for simple, quick operation using a 16-element keypad for push-button tuning. They are capable of short-range or long-range operation for voice or digital data communications. The planning range is 8 to 35 kilometers. They also operate in a jam-resistent, frequency-hopping mode. This can be changed as needed. IHFR is a family of high frequency radios. Radios include the AN/PRC-104 manpack radio and the AN/GRC-193 vehicular radio.

DISCOM HHC/DMMC RADIO NETS

DISCOM COMMAND/ OPERATIONS NET (FM)

The DISCOM command/operations net is the principal net operated by the DISCOM headquarters. See Figure 4-10, page 4-12. This net is a backup to MSE. It is used to command and control elements of the DISCOM in the performance of its logistics mission. The net control station is the S2/S3 section. Stations in this net monitor the division command/operations net and the division intelligence net. This net is also used for rear operations as required.

DISCOM MATERIEL MANAGEMENT NET (FM)

This net supports the technical aspects of logistics support to the division. See Figure 4-11 page 4-13. It maintains continual communications between components of the DMMC for coordination of critical areas (Class I, III, V and maintenance management). The net control stat ion is the DISCOM materiel management office.

Class I and Class III and Water Supply Branch Officers

These branches are subordinate to the general supply section. However, they are also distinct operating entities within the DMMC. The Class I supply branch officer has a radio for Class I operations. The Class III and water supply branch officer has a radio for Class III operations. Each branch uses the mobile station in this net. This is done to coordinate with other DISCOM elements on issue points, problems, shortages, excesses, and requirements. Agents of these branches are constantly traveling within the division and brigade areas to ensure the smooth functioning of their respective supply operations.

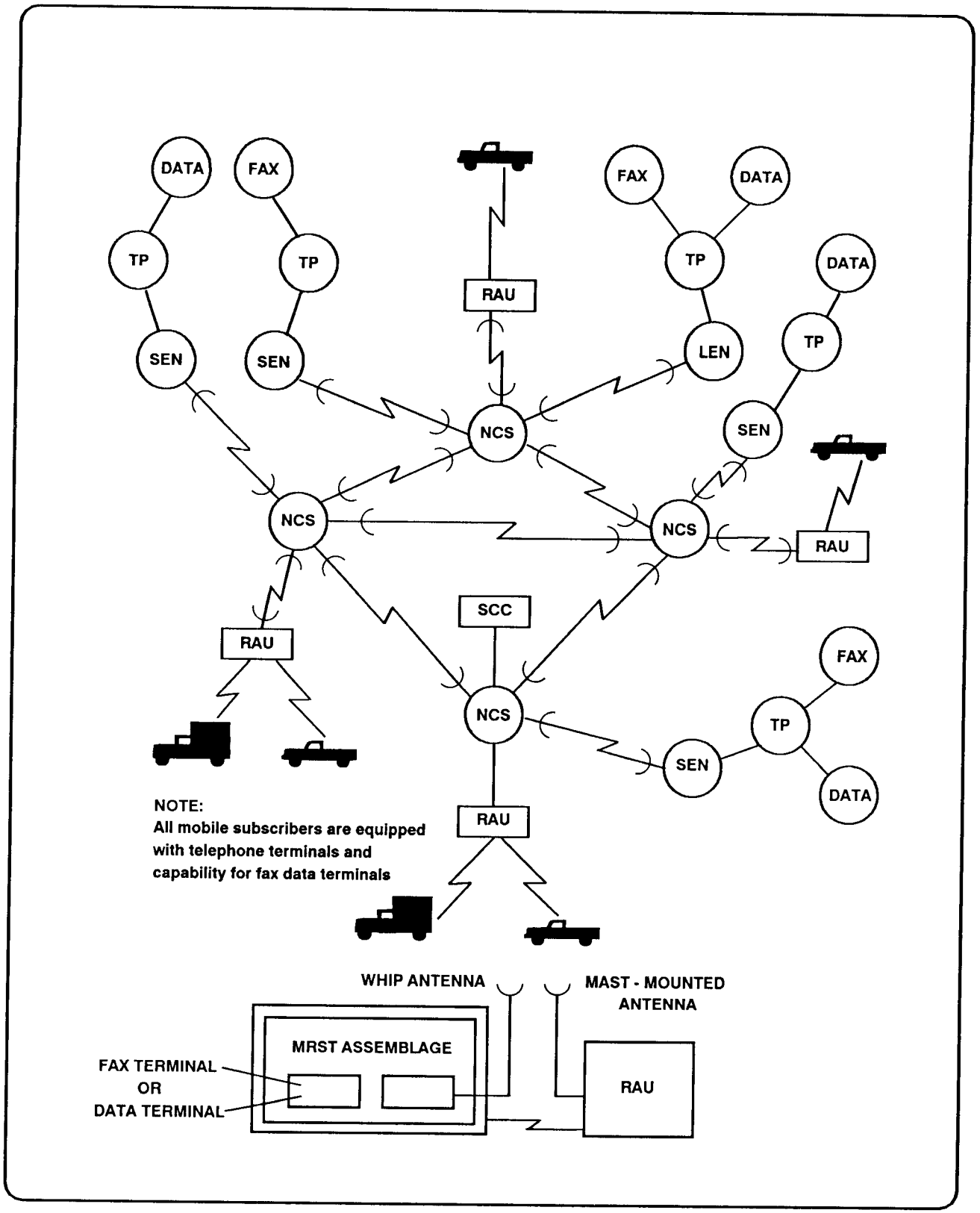

Figure 4-9. Mobile subscriber interface.

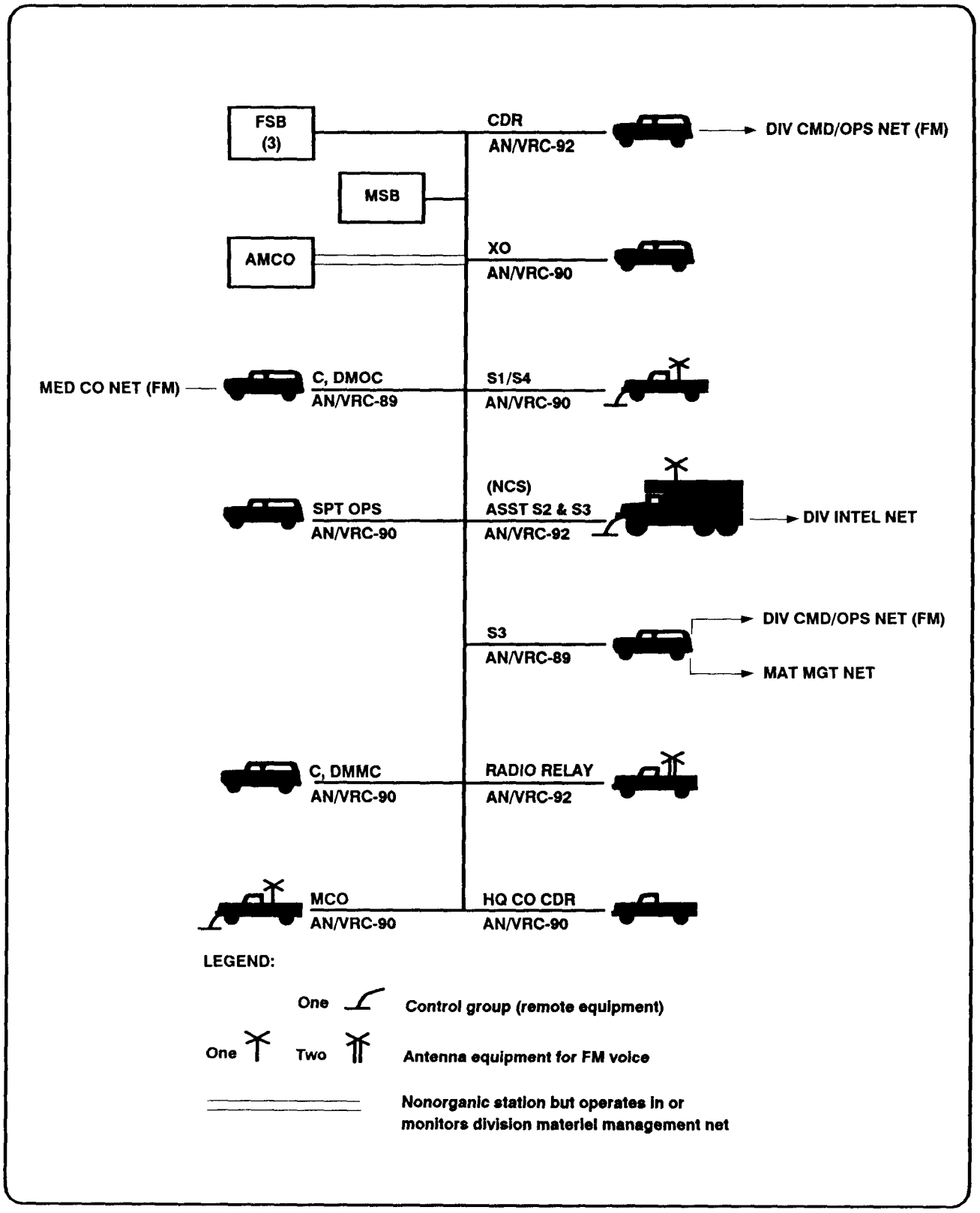

Figure 4-10. Heavy DISCOM command/operations net (FM).

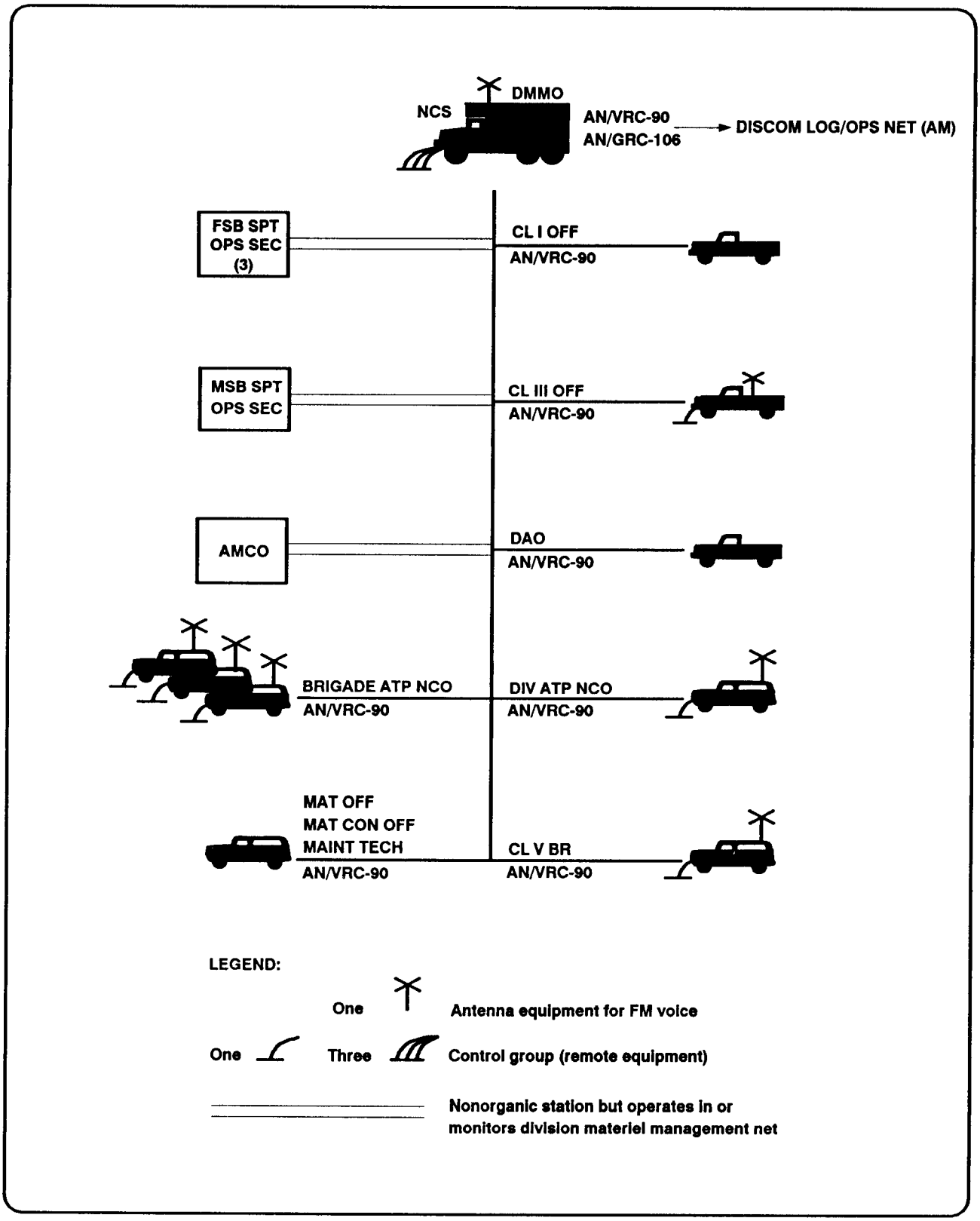

Figure 4-11. DISCOM materiel management net (FM).

Class II-IV Supply Branch Technician

The Class II-IV supply branch technician does not have a radio assigned to the section. He has access to the net by using radios assigned to other branches in the DMMC. The layout of the DMMC will determine which branch radio he will use.

Class V Supply Section Officer

The DAO uses the materiel management net to provide coordination and control necessary to monitor ammunition supply. The DAO uses a mobile station in this net to solve problems while on the move. The DAO must always be able to communicate with the DMMC chief. The DAO communicates with the G3 and the COSCOM MMC Class V section via the area communications system. He communicates with each support battalion via the materiel management net.

Within this net, the DAO has a radio. The ammunition supply technician, the chief ammunition NCO, and the ammunition inspection NCO share a radio. They normally operate from the DMMC field location. The two radios are in separate trucks. These radios provide a communication link with the division and brigade ammunition NCOs located at the ATPs. The ATP NCOs have a radio and can communicate with these two sources for their information and guidance.

Materiel Officer

The materiel officer uses his mobile station in this net to coordinate with the DMMC. This allows for the quick resolution of materiel problems throughout the division.

DISCOM LOGISTICS OPERATIONS NET (AM-SSB)

This net provides along-range command and control link for the DISCOM. This is especially helpful when the division is operating over extended distances. It also provides a long-range link to the COSCOM elements as required. The net control station for this net is the DISCOM support operations branch (Figure 4-12).

DISCOM MEDICAL OPERATIONS NET (AM-SSB)

The chief of the DMOC uses this net to coordinate patient medical regulating, air/ground evacuation, and emergency medical resupply. This coordination is with the division medical companies and corps medical brigade elements (Figure 4-13).

COMSEC

COMSEC consists of measures taken by a unit to prevent unauthorized persons from gaining information of value from communications. It includes crypto-security, physical security, transmission security, and emission security.

Supervisors must prescribe policies and procedures for safeguarding COMSEC materiel during tactical operations. They must also provide instructions for implementing emergency procedures during operations. The responsibility for safeguarding classified COMSEC information rests not only with the commander but with every individual in the command. This especially applies to those people who handle, store, use, or have knowledge of subject information.

The sensitivity of COMSEC information dictates that it be available only to those personnel who have a need to know. A person's office, position, or security clearance does not automatically entitle him access to COMSEC information. However, all personnel who require access to classified COMSEC information must have the appropriate security clearance.

COMSEC materiel must be requested in advance. The COMSEC custodian must be informed at least 24 hours prior to the requested pickup time. Users are issued COMSEC materiel on a SF153 (Hand Receipt).

Hand-receipt holders/users physically verify the serial numbers and quantity of COMSEC materiel they are receiving against the hand receipt. This is done prior to signing for the materiel and ensures there are no discrepancies. These hand-receipt holders cannot and will not subhand-receipt COMSEC materiel they have on hand receipt without prior approval of the COMSEC custodian.

The prompt reporting of physical and cryptographic security violations and compromises is essential to the maintenance of adequate communications security. A compromise results from any occurrence that enables unauthorized persons to derive useful information from encrypted communications.

A compromise may result from either of two types of insecurities. Physical insecurities occur

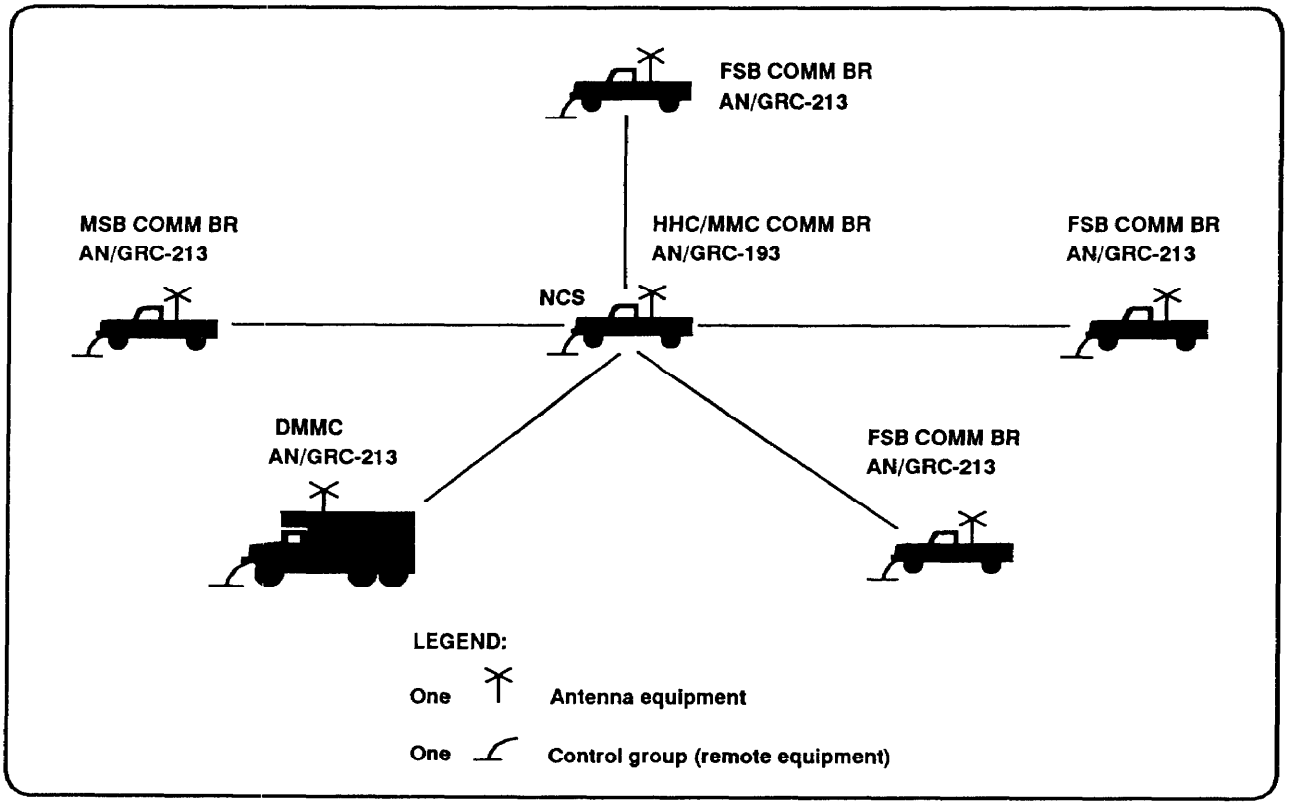

Figure 4-12. DISCOM logistics operations net (AM-SSB).

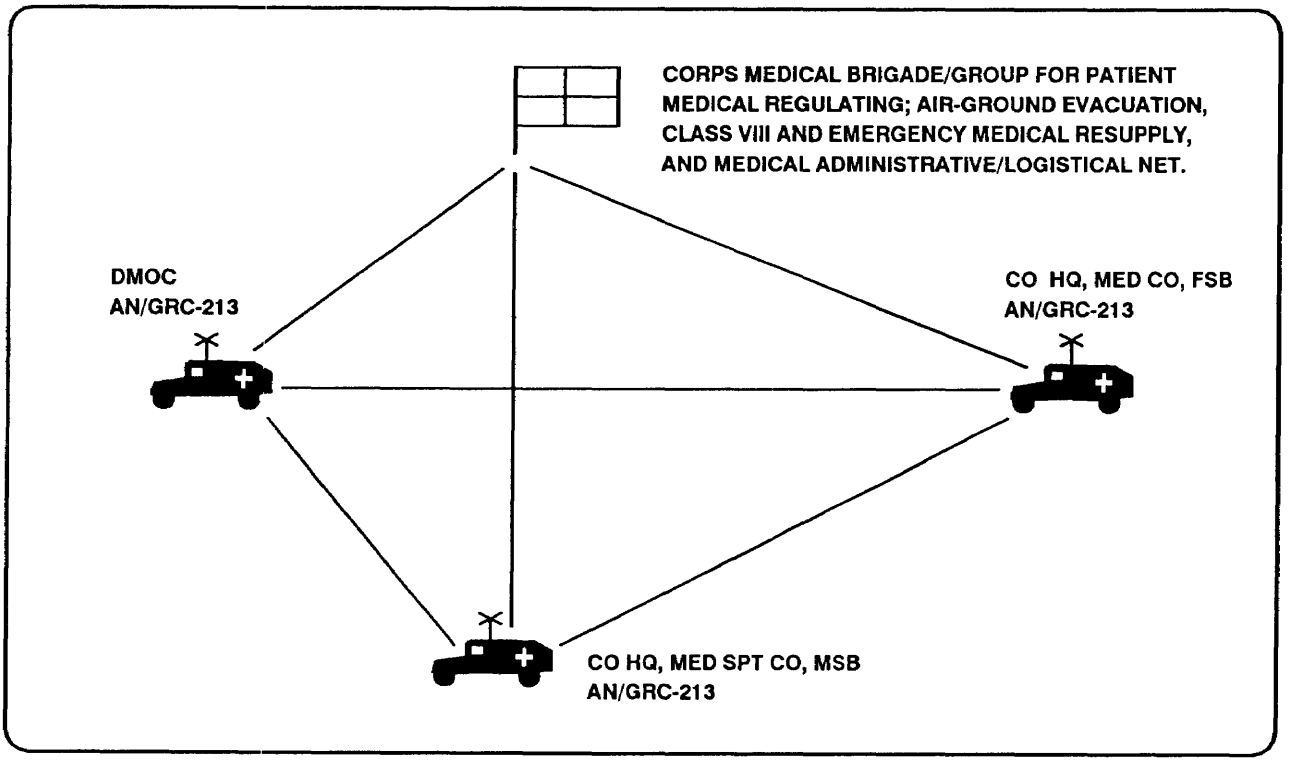

Figure 4-13. DISCOM medical HF voice net.

when classified information is lost or possibly exposed to an unauthorized person. This includes information subject to compromise through personnel insecurities. Personnel insecurities include detection, unauthorized absence, deliberate or inadvertent disclosure to an unauthorized person, and the removal of a security clearance for cause.

Any known or suspected compromise or other security violation must be reported immediately to the commander, COMSEC custodian, or supervisor. He will in turn determine the necessary actions to be taken.

Destroy all superseded COMSEC materiel beyond recognition.

OPSEC

OPSEC deals with protecting friendly military operations and activities by identifying the EEFI and providing appropriate protection to those EEFI. It aids in keeping the enemy from learning how, when, where, and why US forces do something. A basic OPSEC program would consist of four phases.

ESTABLISHING COMMAND'S SECURITY OBJECTIVES AND DEVELOPING ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

Initially, the commander identifies what operations, activities, and projects must not be compromised to ensure accomplishment of his overall mission. These identified areas are translated into the command's security objectives. The CSO are usually stated broad terms (for example, "prevent technology transfer of the...technology"; "achieve surprise fielding of the ...weapon systems"; or "prevent disclosure of the unit's readiness and deployment posture"). CSO properly stated indicate "what we are doing and why we are doing it."

The CSO are used as a basis to develop EEFI. EEFI are specific, critical, and sensitive items of information that individually or collectively need protecting. Protection will preclude the compromise of the CSO. Information such as specific dates, times, locations, intentions, and capabilities may need to be protected.

EEFI can include both classified and sensitive unclassified information. Sensitive, unclassified information is information which could give an insight into an area of classified information or divulge CSO. A combination of more than one piece of sensitive, unclassified information may contain sufficient detail to warrant classification. Disclosure of this sensitive, unclassified information could have negative results on future operations, activities, or projects.

DETERMINING THE POTENTIAL THREAT

The threat is determined by evaluating the capabilities of foreign intelligence services to collect EEFI. The threat profile should evaluate foreign intelligence awareness, their motivation, and their capability to collect information. The profile should also give you what the probability will be of your operation, activity, or project being targeted. Collection of intelligence information by foreign intelligence service is accomplished by a variety of means. The following disciplines normally will be included in a multisource intelligence threat:

- HUMINT is intelligence obtained by using people to gather various items of information. HUMINT collection involves both overt and clandestine operations. Examples of overt operations would include information obtained from public records and unclassified publications and newspapers. Clandestine operations include people eavesdropping on conversations and conducting surveillance or special operations.
- SIGINT is intelligence obtained by intercepting electronic signals. This information is obtained by intercepting telecommunications signals, such as telephone or radio conversations (normally referred to as COMINT). Information also is obtained by intercepting electromagnetic nondata-related radiations, such as radar signals (normally referred to as ELINT). Signal security is an overall term for the security measures taken to deny collection of information from COMINT and ELINT operations.
- IMINT is intelligence obtained through the use of photographic, infrared, or radar imagery equipment. Satellites, aircraft, and land or sea based vehicles/vessels can house imagery equipment. IMINT also can be provided by human sources who employ imagery equipment.

DEVELOPING A UNIT PROFILE

The unit OPSEC officer works with the CI section to develop a unit profile. With a profile, the OPSEC officer can determine what information a foreign

intelligence service might collect. This profile allows a unit to see itself as the enemy would see it. A profile consists of patterns and signatures, Patterns are stereotyped actions which so habitually occur in a given set of circumstances that they cue an observer (foreign intelligence service). So habitual are these actions, that the observer is able to determine the type operation/activity/project, its capabilities, or its intent. Signatures provide the identification of the operation/activity/project. Signatures result from unique visual (imagery), electromagnetic, olfactory, or sonic displays. A unit profile is developed by a team. The team should observe every facet of the operation to identify patterns and signatures. The team members should be knowledgeable in specific aspects of the operation/a ctivity/project. Separate profiles should be developed for the following areas: operations/maneuvers, communications/electronics, intelligence, logistics, and administration/support.

ASSESSING VULNERABILITIES

Once the threat is identified and a profile developed, a risk assessment is prepared. The assessment centers on the operation/activity/project's vulnerability to collection. All EEFI must be considered in this assessment. The assessment considers numerous factors. Examples of some factors are the project sensitivity, or the known, or suspected collection priority by foreign intelligence service. The operating environment, the proximity to international borders, and security programs are some additional factors. Security education as well as physical and natural barriers are also factors to be considered. An assessment of where, how, and why an operation/activity/project is vulnerable naturally leads to recommendations on how to reduce these vulnerabilities.

A countermeasure is any action taken to eliminate or reduce a vulnerability to collection. When recommending countermeasures, planners should consider on-the-spot corrections which effectively minimize or neutralize identified vulnerabilities. Low cost/no cost solutions must be sought and emphasized. Such recommendations may be of a temporary or permanent nature. Temporary recommendations to neutralize a vulnerability usually relate to an event. When the event takes place, further action is no longer required. Where extensive corrections must be taken or high costs are involved, recommendations should be prioritized to permit an incremental approach for adoption that is phased over a period of time. A commander's decision on what countermeasures to implement relate directly to risk versus cost benefit.

Principal components of any OPSEC program include physical security, information security, signal security, security education, and at times, deception operations.

Physical security measures may include a badge and pass system, security guards, and perimeter fencing. Such measures should be included, as appropriate, when you develop your OPSEC program. A good reference for physical security is FM 19-30.

Information security is also of vital importance to the OPSEC program. Security procedures, such as using only approved storage containers, double-checking offices prior to departure, and ensuring the "need-to-know," are measures that can be taken to protect classified and sensitive, unclassified information. AR 380-5 contains important provisions dealing with information security.

SIGSEC includes all measures taken to deny collection of information from both COMINT and ELINT operations. Something as simple as not discussing classified or sensitive, unclassified information over the telephone can greatly assist in maintaining the security of an operation, installation, or activity.

Security education consists of initial security orientations, refresher briefings, foreign travel briefings, and debriefings. The focus of the training and education program is to highlight to all personnel, the threat that exists to classified and sensitive, unclassified information. The program also provides measures to be taken to reduce that threat to the lowest practical level. One objective of any security education program is to convince the individual that this is information he needs to learn. Without an awareness of the need for security on the part of all personnel, other security measures, such as fences, guards, and alarms, are reduced in effectiveness.

AUTOMATION SYSTEMS SECURITY

Automated systems are vulnerable to destruction, sabotage, and compromise. Security includes not only physical security of hardware devices but security of programs and procedures. Detailed guidance on

automated systems security is provided in AR 380-380. The following physical and security practices must be established for use of TACCS or other microcomputers –

- Locate the computer within an enclosure that provides controlled access.
- Secure all electrical facilities that support the system.
- Store magnetic media storage containers at least 20 inches from an exterior wall. (This helps provide protection against the potential effects of magnetic fields or radiation.)
- Restrict physical access to magnetic diskettes.
- Require that authorized operators have at least an interim confidential security clearance.
- Restrict access to the computer site by the use of classified passwords.
- Rotate unique operator passwords every 30 days or less.
- Control all log-ons and file access by unique operator passwords.
- Monitor device usage.
- Restrict the access of visitors.
- Monitor report distribution plans.
- Reduce the number of copies of each report.
- Destroy all printouts of reports and lists as new ones are printed.